International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 149-158

TRANS STELLAR
• Journal Publications • Research Consultancy

SECURED STEGANOGRAPHY MODEL USING GENETIC ALGORITHM

AKANKSHA GAUR, PRIYANKA WADHWANI & VIPIN JAIN

Department of Computer Engineering, Swami Keshwanand Institute of Technology, Rajasthan Technical University, Jaipur, India

ABSTRACT

This paper intends to administer an outline of image steganography. It additionally makes an attempt to spot the wants of an honest steganographic rule and in brief reflects on that steganographic techniques. The web as an entire doesn't use secure links; therefore info in transit is also prone to interception additionally. Besides the concealment of information for confidentiality; this approach of knowledge concealment will be extended to copyright protection for digital media. During this analysis, we specialize in the smallest amount vital Bit (LSB) technique out of sight messages in a picture. The system increased the LSB technique by arbitrarily dispersing the bits of the message within the image and therefore creating it more durable for unauthorized individuals to extract the initial message. We tend to build a secured steganography model here that uses the idea of genetic rule, whole number to whole number moving ridge remodel, and best pixel adjustment method to cover the text behind the colour image.

KEYWORDS: Steganography, Concealment; Genetic

INTRODUCTION

One of the explanations that intruders will be sure-fire is that the majority of the data they acquire from a system is in an exceedingly type that they will browse and comprehend. Intruders might reveal the data to others, modify it to misrepresent a personal or organization, or use it to launch an attack. One resolution to the current downside is, through the utilization of steganography. Steganography may be a technique of activity info in digital media. In distinction to cryptography, it's to not keep others from knowing the hidden info however it's to stay others from thinking that the data even exists.

The word steganography comes from the Greek *Steganos*, which implies coated or secret and *–graphy* means writing or drawing. Therefore, steganography suggests that, accurately, coated writing. Steganography is that the art and science of activity info specified its presence can't be detected [1]. Secret info is encoded in an approach specified the existence of the data is hidden in an exceedingly human perceptible.

The main goal of steganography is to speak firmly in an exceedingly undetectable manner [2] and to avoid drawing suspicion to the transmission of hidden information [3]. Therefore, in existing communication strategies, steganography will be accustomed to hidden exchanges. The thought of steganography is to stay others from thinking that the info even exists and to not keep others from knowing the hidden information. If a steganography methodology causes anybody to suspect there's a secret data in a carrier medium, then the tactic has unsuccessful [4].

A stego-system encoder will be depicted by victimization the subsequent relation [6]:

$I' = f(I, m, k)$

Where,

I' is the stego-object

I is the cover-object

m is the message

k is the stego-key.

In general, the data concealing method extracts redundant bits from cover-object. The method consists of 2 steps [7, 8]:

- Identification of redundant bits.
- Embedding method.

Steganographic Techniques

Over the past few years, various steganography techniques that implant hidden messages in multimedia system objects are projected [10]. There are several techniques for concealing information or messages in pictures in such a fashion that the alterations created to the image are perceptually indiscernible. Common approaches are embodying [11]:

- Least vital bit insertion (LSB)
- Masking and filtering
- Rework techniques

PROPOSED WORK

An information hiding system has been developed for confidentiality. However, in this paper, we tend to study a picture file as a carrier to cover message. Therefore, the carrier is going to be referred to as cover-image, while the stego-object referred to as stego-image. The implementation of system can only focus on Least significant Bit (LSB) united of the steganography techniques. The main idea behind this presented technique is to establish robust steganography architecture which defeats RS-attacks by using Genetic algorithm.

In this method for hiding purpose we use a genuine image that is noise free and standard image. Behind this image we embed a message that can be in may lines of sentence. After embed the message the image send to the receiver. In between the communication between the sender and receiver many people over the network i.e. hackers are interested to know that what is actually sent by the sender. So the main advantage of this type of secures technique is that it does not make any type of attention about the message to hackers. The proposed method also restrict the strongest steganalysis method that one known as the RS analysis.

For embedding the info into a picture, we need two important files, first is the original image known as the cover-image. The image in gif format can hold the hidden information. The second file is the message itself that is the info to be hidden within the image.

Before embedding method, the dimensions of image and also the message must be defined by the system. It is important to make sure the image should support the message to be embedded. The best image size is 800*600 pixels, which might engraft up to 60kB messages.

The cover-image is going to be combined with the message. This can manufacture the output known as stego-image. The Stego-image looks clone of the cover-image. However, there are hidden messages that are useable.

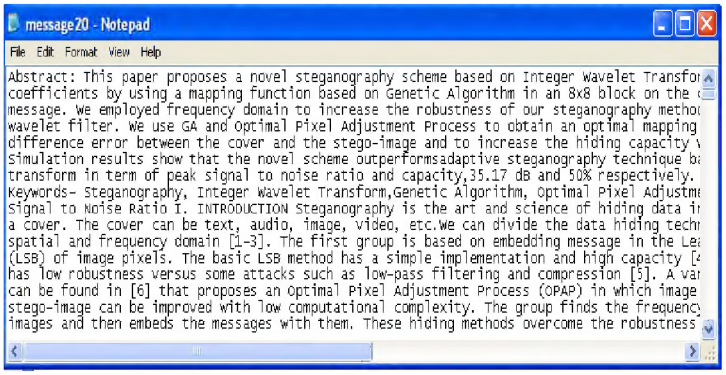

Figure 2.1: Message

This process merely embedded the message into the cover-image while not equipped any arcanum or stego-key. At this stage, we set to do so as a result of we have to grasp the ways in which of LSB insert the message bit into the image and extract the message from the stego-image created.

Figure 2.2: Cover Image (Original)

Figure 2.3: Result of Stego-Image

The advantages of LSB are its simplicity to enter the bits of the message directly into the LSB plane of cover-image and many techniques use these methods [2]. Modulating the LSB does not lead to a human-perceptible difference as a result of the amplitude of the change is small. Therefore, to the human eye, the ensuing stego-image (Figure 2.3) can look the image of the cover-image (Figure 2.2). This permits high perceptual transparency of LSB.

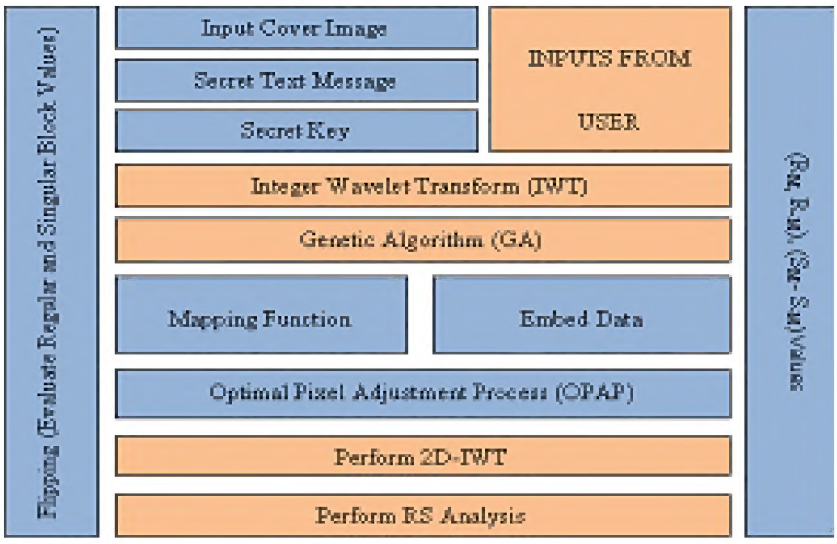

Figure 2.4: Proposed System Architecture

Genetic Algorithm

Genetic Algorithms area unit the heuristic search and optimization techniques that mimic the process of natural evolution. "Select the simplest, Discard the Rest"

The genetic algorithmic program process is kind of simple; it only involves a replica string, partial string exchanges or a string mutation, all these in random type.

IMPLEMENTATION AND RESULT DISCUSSIONS

The appearance of the Internet is considered to be one of the major events of the past years; information become available on-line, all users who have a computer can easily connect to the Internet and search for the information they want to find. This increasing dependency on digital media has created a strong need to create new techniques for protecting

these materials from illegal usage. One of those techniques that have been in practical use for a very long time is Encryption. The basic service that cryptography offers is the ability of transmitting information between persons in a way that prevents a third party from reading it.

The Proposed Algorithm

The introduction of wavelet transforms that map integers to integers in the field of image steganography allowed the embedded message to be recovered without loss. We will apply the 2D *STransform* on each color plane of the colored cover image. Then the proposed algorithm stores the message bit stream in the least significant bits of the transform coefficients. This process obviously does not affect the integrability of the embedded coefficients.

The main problem encountered in implementing this algorithm was the error caused by hiding bits in coefficients that correspond to saturated pixel components. The embedding process may modify those coefficients making them exceed their maximum value (255). This range violation may result in losing some parts of the embedded message. So, we proposed applying a pre-processing step on the cover image before the embedding process takes place. This step adjusts the saturated pixel components in a way to guarantee that they do not exceed their maximum value due to modifying their corresponding coefficients.

Proposed Method Implementation in MATLAB

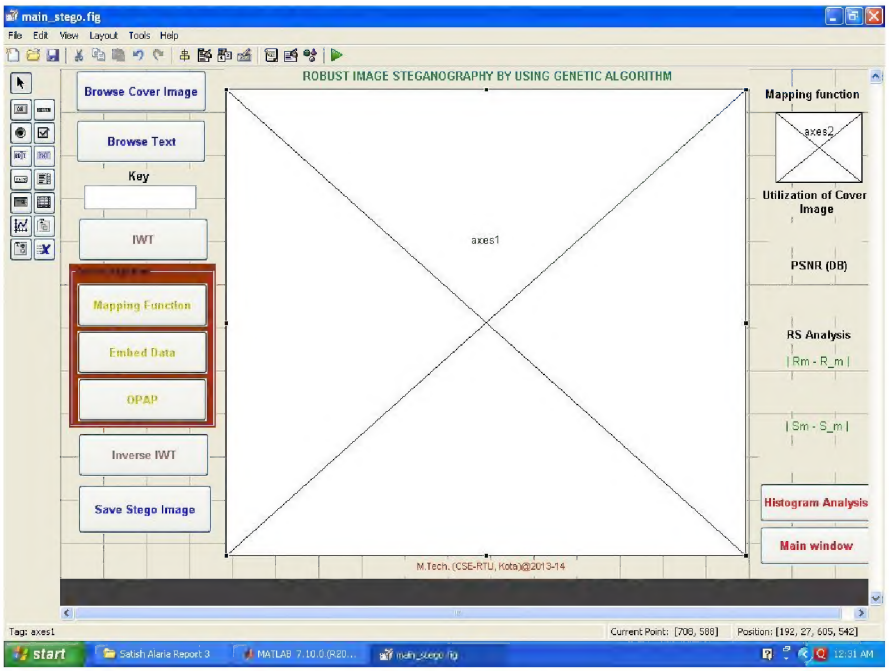

Figure 3.1: Main Stego in MATLAB

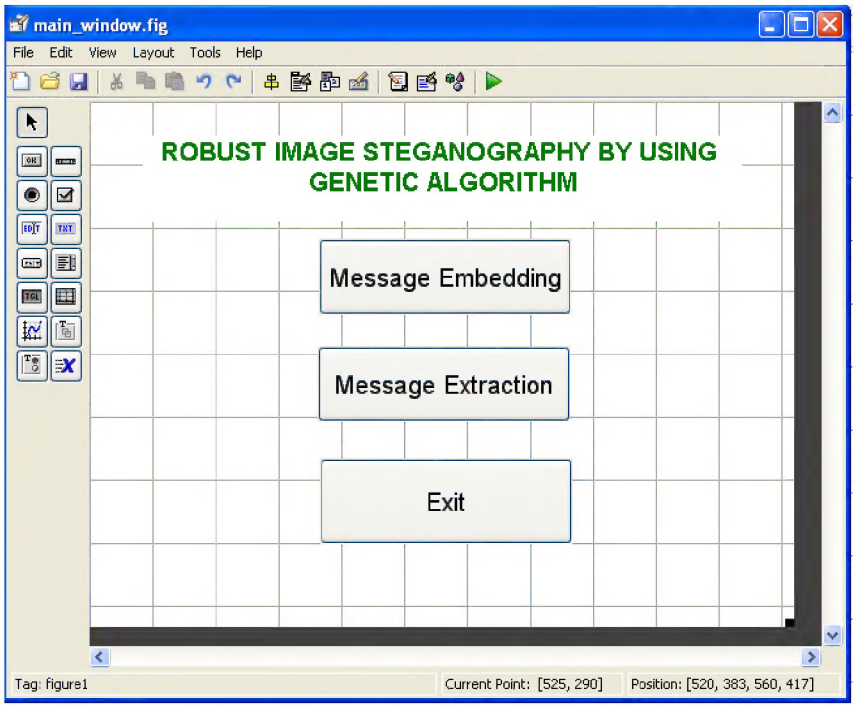

Figure 3.2: Main Window in MATLAB

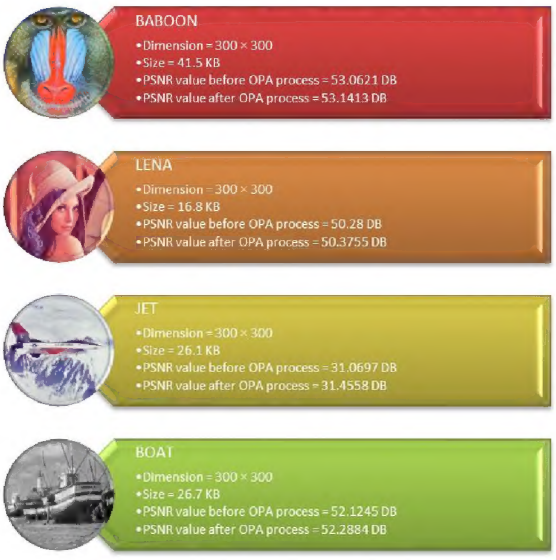

Figure 3.3: Image Comparison Based on Size and PSNR Value When Dimension 300 × 300 And K=4

Figure 3.4: RS Analysis Value Comparison for 300 × 300 Dimensions and K=4

CONCLUSIONS

We pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A *stego-key* has been applied to the system during embedment of the message into the cover-image. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Finally, we have shown that steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message.

Presented work presents a highly secured and robust steganography idea to increase the hiding capacity and PSNR value after embedding the data in cover image. Generally by the previous existing all techniques the image quality was degrades as we increase the capacity of hiding material but by the present technique we achieve 100% utilization of cover image as well as maintain the overall image quality. In this proposed work genetic algorithm is applied to maintain the local image properties. The pixel values of the stego image are modified by this algorithm to maintain their statistical characteristics. So by this attacker are in deep trouble for detect the existence of the secret message by using the RS analysis technique. We also applied the OPAP to reduce the distortion in the stego image as compared to the cover image. The OPA process also increases the hiding capacity of image by the pixel adjustment in suitable place.

Wavelet transforms that map integers to integers allow perfect reconstruction of the original image. The proposed algorithm deals with true-color images. The embedding process stores up to 3 to 6 message bits in each integer coefficient for all the transform sub-bands.

The algorithm pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. The information capacity provided by the proposed algorithm can reach 50% of the original cover image size. Furthermore, experimental results showed that this scheme retains high quality of the stego-image over the existing LSB-based methods.

Recommended Guidelines Future Work

The knowledge of the technology is still limited to mainly the research individuals and academia; however there is a growing understanding that this technology could be used widely. UTM should carry out more research into the field of information hiding. In future, we would extend the system to be more robust and efficient. The research will include the enhancement of the algorithm that will utilize the entire image for embedding the message. We will also analyze the processing time to generate the random number and introduce method(s) to minimize the time.

As we increase the length of the secret data, the chance of detection of secret hidden message by attackers also increases. Future works focus upon the length problem as well as on histogram attack.

ACKNOWLEDGEMENTS

Through this page, I express my heartfelt thanks, to Mr. Vipin Jain (Senr. Lect.), Computer Science Department at Swami Keshvanand Institute of Technology, Management and Gramothan Jaipur, who gave me the opportunity to work on this topic and inspired me to carry forward this work as a challenge.

REFERENCES

1. C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
2. R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001
3. N.F. Johnson, S. Jajodia, "Staganalysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 1998.
4. D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-Jun 2001.
5. R A Isbell, "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, 10 May 2002.
6. R. Popa,"An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.
7. N. Provos, P. Honeyman, "Detecting Steganography Content on the Internet". CITI Technical Report 01-11, 2001.
8. N. Provos, "Probabilistic Methods for Improving Information Hiding", CITI Technical Report 01-1, January 31, 2001.
9. M. Ramkumar & A.N. Akansu. "Some Design Issues For Robust Data hiding Systems", <http://citeseer.nj.nec.com/404009.html>
10. N.F. Johnson & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", in Proceeding for the Second Information Hiding Workshop, Portland Oregon, USA, April 1998, pp. 273-289.
11. N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34, 1998.
12. R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Area in Communications, pp. 474-481, May 1998.

13. S. Tanako, K. Tanaka and T. Sugimura, "Data Hiding via Steganographic Image Transformation", IEICE Trans. Fundamentals, vol. E83-A, pp. 311-319, February, 2000.
14. F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in proceeding of IEEE, pp. 1062-1078, July 1999.
15. M.M. Amin, M. Salleh, S. Ibrahim, et al., "Information Hiding Using Steganography", 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, pp. 21-25, January 14-15, 2003.
16. P. Moulin & J.A. O'Sullivan, "Information – Theoretic Analysis of Information Hiding", at IEEE International Symposium on Information Theory, Boston, MA, October, 1999.
17. J. Zollner, H. Federrath, H. Klimant, et al., "Modeling the Security of Steganographic Systems", in 2nd Workshop on Information Hiding, Portland, April 1998, pp. 345-355.
18. E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99, Ed., Apr. 1999, pp. 274--278.
19. N. Provos and P. Honeyman. "Hide and Seek: An Introduction to Steganography", IEEE: Security & Privacy, vol. 1, pp. 32-44, 2003.
20. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. "Digital Watermarking and Steganography (Second Edition)", Morgan Kaufmann Publishers, ISBN: 978-0-12- 372585-1, 2007.
21. J. Fridrich, M. Goljan, and D. Hogea. "Attacking the OutGuess", Proceedings of the3rd Information Hiding Workshop on Multimedia and Security 2002, Juan-les-Pins, France, 2002
22. C. Stanley. "Paris of Values and the Chi-squared Attack", Master's thesis, Department of Mathematics, lowa State University, 2005.
23. C. Darwin, The Origin of the Species, Cambridge, Ma., Harvard University Press, 1967.
24. R.A. Fisher, The Genetical Theory of Natural Selection. Clarendon press, Oxford 1930.
25. A.D. Channon, and R.I. Damper, "Towards the Evolutionary Emergence of Increasingly Complex Advantageous Behaviours". International Journal of Systems Science, 31(7), pp. 843-860, 2000.
26. Carlos D. Toledo, "Genetic Algorithms for the numerical solutions of variational problems without analytic trial functions", arXiv:Physics/0506188, pp. 1-3, June 2005.
27. J. Holland, "Genetic Algorithms" Sci. Am. pp.114-116, 1992.
28. T. Bäck and H. P. Schwefel, "An Overview of Evolutionary Algorithms" Evolutionary Comput. 1: pp. 1-23, 1993.
29. Allen B. Tucker (Jr.), The Computer Science and Engineering Handbook, CRC Press, USA, pp. 557-571, 1997.
30. J.H. Holland, Adaptive in Natural and Artificial Systems. Ann Arbor, MI: University of Michigan Press, 1975.
31. D.E. Goldberg, Genetic Algorithms, in Search, Optimization & Machine Learning. Addison Wesley, 1997.

32. T. Bäck, Evolutionary Algorithms in Theory and Practice: Evolution Strategies, Evolutionary Programming, Genetic Algorithms. Oxford University Press, N.Y.,1996

33. K. Solanki, A. Sarkar, and B. Manjunath. "YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis", Lecture Notes in Computer Science, vol. 4567, pp. 16-31, 2008.

34. D. Cvetkovic, and H. Muhlenbein, "The Optimal Population Size for Uniform Crossover and Trucation Selection", Technical Report GMD-AS-TR-94-11, 1994.

35. K.A. De Jong and W.M. Spears, "An Analysis of Interacting Roles of Population Size and Crossover in Genetic Algorithms", Proceedings of the international Conference on Parallel Problems Solving from Nature (eds. Schwefel, H.P. & Manner, R.), Springer-Verlag, pp. 38-47, 1990.

36. H.P. Schwefel, Numerical Optimization of Computer Models, John Wiley & Sons, New York, 1981.

37. J.J. Grefenstette, "Optimization of Control Parameters for Genetic Algorithms". IEEE Trans on Systems, Man and Cybernetics. Vol. 16, N°.1, pp 122-128, 1986.

38. Y. Rahmat-Samii, and E. Michielssen, Electromagnetic Optimization by Genetic Algorithms, John Wiley & Sons, 1999.

39. D.S. Weile, and D.E. Goldberg, "Genetic Algorithm design of Pareto Optimal Broad Band Microwave Absorbers", IEEE Transactions on Electromagnetic Compatibility, Vol. 38, pp. 518-524, 1996.